BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-164656
(43)Date of publication of application : 19.06.1998

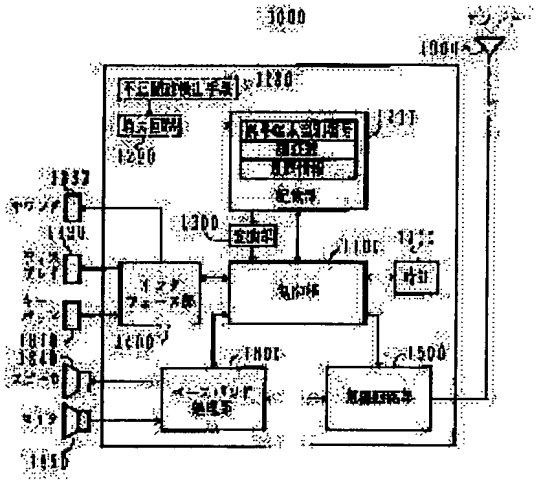
(51)Int.Cl. H04Q 7/38
H04L 9/08
H04L 9/14
H04M 1/66
H04M 3/22

(21)Application number : 08-314733
(22)Date of filing : 26.11.1996

(71)Applicant : HITACHI LTD
(72)Inventor : KOIDE AYUMI
KITAMURA YOICHI

(54) PORTABLE TERMINAL, MANAGING CENTER THEREFOR AND SUPERVISORY AND CONTROL PART THEREFOR

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a portable terminal, portable terminal managing center and supervisory and control part of the terminal hardly performing unauthorized speaking by generating a new certificate key based on a certificate key and history information, using the new certificate key, converting certificate data sent from a base station into certificate response data and transferring the data to the base station.
SOLUTION: A control part 1100 of portable terminal 1000 performs entire control or history information calculation/storage, etc. A storage part 1200 stores portable terminal identification numbers, fixed certificate keys and history information or the like of respective registered portable terminals. Based on the fixed certificate keys and history information stored in the storage part 1200, a converting part 1300 generates the new certificate key. In the case, since the history information is successively reloaded at the time point of speaking end, the newly generated certificate key becomes a successively variable certificate key so as to be hardly illegally acquired.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－164656

(43)公開日　平成10年(1998)６月19日

(51)Int.Cl.⁶		識別記号	FI		
H04Q	7/38		H04B	7/26	109R
H04L	9/08		H04M	1/66	B
	9/14			3/22	Z
H04M	1/66		H04L	9/00	601B
	3/22				641

審査請求　未請求　請求項の数７　ＯＬ　（全 11 頁）

(21)出願番号　特願平8－314733

(22)出願日　平成８年(1996)11月26日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

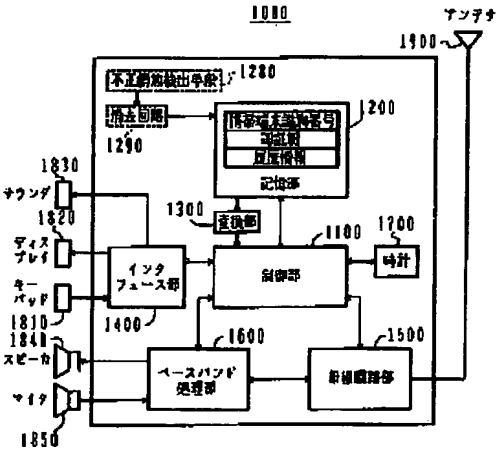
(72)発明者　小出　歩
神奈川県横浜市戸塚区戸塚町216番地　株式会社日立製作所情報通信事業部内

(72)発明者　北村　洋一
神奈川県横浜市戸塚区戸塚町216番地　株式会社日立製作所情報通信事業部内

(74)代理人　弁理士　春日　譲

(54)【発明の名称】　携帯端末及び携帯端末の管理センタ及び携帯端末の監視制御部

(57)【要約】
【課題】本発明の目的は、不正通話の行い難い携帯端末及び携帯端末の管理センタ及び携帯端末の監視制御部を提供することにある。
【解決手段】携帯端末１０００は、携帯端末識別番号と携帯端末毎に予め与えられている認証鍵と携帯端末の過去の使用状況を示す履歴情報とを記憶する記憶部１２００と、この記憶部１２００に記憶された認証鍵と履歴情報に基づいて新たな認証鍵を生成する変換部１３００と、この変換部１３００によって生成された新たな認証鍵を用いて、基地局２１００から送られてきた認証データを認証応答データに変換する制御部１１００とから構成されている。



1

【特許請求の範囲】

【請求項１】　携帯端末識別番号と携帯端末毎に予め与えられている認証鍵と携帯端末の過去の使用状況を示す履歴情報とを記憶する記憶部と、

この記憶部に記憶された上記認証鍵と上記履歴情報に基づいて新たな認証鍵を生成する変換部と、

この変換部によって生成された新たな認証鍵を用いて、基地局から送られてきた認証データを認証応答データに変換する制御部とを備え、

この制御部で変換された認証応答データを上記基地局に転送することを特徴とする携帯端末。

【請求項２】　請求項１記載の携帯端末において、

上記記憶部に記憶されている履歴情報は、過去の通話回数、過去の通話開始時間、過去の通話終了時間、過去の通話時間、及び過去の通話位置からなることを特徴とする携帯端末。

【請求項３】　請求項１記載の携帯端末において、さらに、

上記記憶部を内蔵する筐体の不正開放を検出する不正開放検出手段を備え、

この不正開放検出手段による筐体の不正開放の検出信号に基づいて、上記記憶部の記憶内容を消去することを特徴とする携帯端末。

【請求項４】　携帯端末識別番号と携帯端末毎に予め与えられている認証鍵と携帯端末の過去の使用状況を示す履歴情報とを記憶する記憶部と、

この記憶部に記憶された上記認証鍵と上記履歴情報に基づいて新たな認証鍵を生成する変換部と、

この変換部によって生成された新たな認証鍵を用いて、認証データを認証応答データに変換するとともに、携帯端末から送られてきた認証応答データと比較して、両者が一致した場合に、通話を許可する制御部とを備えたことを特徴とする携帯端末の管理センタ。

【請求項５】　請求項４記載の携帯端末の管理センタにおいて、

上記記憶部に記憶されている履歴情報は、過去の通話回数、過去の通話開始時間、過去の通話終了時間、過去の通話時間、及び過去の通話位置からなることを特徴とする携帯端末の管理センタ。

【請求項６】　携帯端末毎に通話料金の上限値を記憶する記憶部と、

この記憶部に記憶された上記通話料金の上限値を越えた場合に、管理センタに携帯端末の停止命令のコマンドを送る制御部とを備えたことを特徴とする携帯端末の監視制御部。

【請求項７】　携帯端末の過去の通話開始時間と過去の通話位置を記憶する記憶部と、

この記憶部に記憶された過去の通話開始時間と過去の通話位置の情報に基づいて、一定時間内に、通話位置が前回の通話位置から予め設定しておいた距離以上である場合、管理センタに、携帯端末の停止命令のコマンドを送る制御部とを備えたことを特徴とする携帯端末の監視制御部。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、携帯端末及び携帯端末の管理センタ及び携帯端末の監視制御部に係り、特に、クローニング対策を講じた携帯端末及び携帯端末の管理センタ及び携帯端末の監視制御部に関する。

【０００２】

【従来の技術】携帯端末を用いる無線通信システムにおいては、無線区間で他人の携帯端末のＩＤ等の識別番号を盗み出し、自身の携帯端末に盗み出したＩＤ等の識別番号を書き込むことによって他人に成りすまし、他人の課金で携帯端末を利用するクローニングによる被害が問題になっている。

【０００３】このような不正な携帯端末による使用を防止するため、従来は、例えば、斉藤、立川著「移動通信ハンドブック」、オーム社、ｐ．１５２に記載されているように、各携帯端末毎に、予め携帯端末に固有の認証鍵を割り当てるようにしていた。

【０００４】携帯端末は、基地局に接続するため、基地局に対してサービス要求を送出する。基地局は、認証を行うために必要な認証用乱数Ｒを生成し、認証用乱数を携帯端末に伝送する。携帯端末は、認証用乱数を携帯端末毎に割り当てられている認証鍵を用いて、認証応答データに変換し、基地局に送り返す。基地局は、携帯端末から送られてきた認証応答データと基地局内で予め求めておいた認証応答データを比較して、両者が一致する場合にのみ、接続を許可するようにしている。正当な携帯端末でない場合には、携帯端末毎に対応する認証鍵を持っていないので、認証応答データへの変換が正しく行われないため、基地局は接続を拒否することになる。このような認証方法を用いることによって、基地局は、不当な携帯端末をチェックするようにしているものである。

【０００５】

【発明が解決しようとする課題】従来の端末認証は、各携帯端末毎に、予め割り当てられていた固有の認証鍵を用いるため、この認証鍵が知られてしまった場合、別の携帯端末のＲＯＭ等の記憶装置に認証鍵をインプットするだけで、クローン携帯端末を簡単に作成できる。従って、このようなクローン携帯端末を使用して、他人を装って、他人の料金で不正通話を行う場合が生じるという問題があった。

【０００６】本発明の目的は、不正通話の行い難い携帯端末及び携帯端末の管理センタ及び携帯端末の監視制御部を提供することにある。

【０００７】

【課題を解決するための手段】上記目的を達成するために、本発明は、携帯端末識別番号と携帯端末毎に予め与

えられている認証鍵と携帯端末の過去の使用状況を示す履歴情報とを記憶する記憶部と、この記憶部に記憶された上記認証鍵と上記履歴情報に基づいて新たな認証鍵を生成する変換部と、この変換部によって生成された新たな認証鍵を用いて、基地局から送られてきた認証データを認証応答データに変換する制御部とを備え、この制御部で変換された認証応答データを上記基地局に転送するようにしたものであり、かかる構成により、認証鍵が逐次更新されるため、不正使用を行い難くなるものである。

【０００８】上記携帯端末において、好ましくは、上記記憶部に記憶されている履歴情報は、過去の通話回数，過去の通話開始時間，過去の通話終了時間，過去の通話時間，及び過去の通話位置から構成したものである。

【０００９】上記携帯端末において、好ましくは、さらに、上記記憶部を内蔵する筐体の不正開放を検出する不正開放検出手段を備え、この不正開放検出手段による筐体の不正開放の検出信号に基づいて、上記記憶部の記憶内容を消去するようにしたものである。

【００１０】上記目的を達成するために、本発明は、携帯端末識別番号と携帯端末毎に予め与えられている認証鍵と携帯端末の過去の使用状況を示す履歴情報とを記憶する記憶部と、この記憶部に記憶された上記認証鍵と上記履歴情報に基づいて新たな認証鍵を生成する変換部と、この変換部によって生成された新たな認証鍵を用いて、認証データを認証応答データに変換するとともに、携帯端末から送られてきた認証応答データと比較して、両者が一致した場合に、通話を許可する制御部とを備えるようにしたものであり、かかる構成により、認証鍵が逐次更新されるため、不正使用を行い難くなるものである。

【００１１】上記携帯端末において、好ましくは、上記記憶部に記憶されている履歴情報は、過去の通話回数，過去の通話開始時間，過去の通話終了時間，過去の通話時間，及び過去の通話位置から構成したものである。

【００１２】上記目的を達成するために、本発明は、携帯端末毎に通話料金の上限値を記憶する記憶部と、この記憶部に記憶された上記通話料金の上限値を越えた場合に、管理センタに携帯端末の停止命令のコマンドを送る制御部とを備えるようにしたものであり、かかる構成により、通話料金が上限値を越えたか否かに基づいて、容易に不正使用を判断し得るものとなる。

【００１３】上記目的を達成するために、本発明は、携帯端末の過去の通話開始時間と過去の通話位置を記憶する記憶部と、この記憶部に記憶された過去の通話開始時間と過去の通話位置の情報に基づいて、一定時間内に、通話位置が前回の通話位置から予め設定しておいた距離以上である場合，管理センタに、携帯端末の停止命令のコマンドを送る制御部とを備えるようにしたものであり、かかる構成により、通話位置と時間の情報により、

容易に不正使用を判断し得るものとなる。

【００１４】

【発明の実施の形態】以下，図１～図５を用いて，本発明の一実施形態による携帯電話システムについて説明する。最初に、図１を用いて，本発明の一実施形態による携帯電話システムの全体構成について説明する。図１は，本発明の一実施形態による携帯電話システムのブロック図である。

【００１５】携帯電話システムは、複数の携帯端末１０００－１，１０００－２，１０００－３と、複数の基地局２１００－１，２１００－２，２１００－３と，交換制御局２２００と、管理センタ２３００と、監視制御部２４００とから構成されている。

【００１６】複数の携帯端末１０００－１，１０００－２，１０００－３は、それぞれ、移動可能であり，通話時には、最も近接する基地局２１００－１，２１００－２，２１００－３との間で，無線通信により接続される。交換制御局２２００は，一方では，公衆網３１００を介して複数の電話機３２００や他の通信機器に接続され，他方では，基地局２１００－１，２１００－２，２１００－３に接続されており、所望の携帯端末１０００－１，１０００－２，１０００－３と所望の電話機３２００間の交換制御を行うものである。

【００１７】管理センタ２３００は，その内部に認証手段を備えており，この認証手段は，携帯端末１０００－１，１０００－２，１０００－３が正当な使用であるか否かを判定を行い、正当な使用であると判定された場合には，交換制御局２２００に対して接続を許可し，不正使用であると判定された場合には，交換制御局２２００に対して接続を拒否するものである。管理センタ２３００の詳細構成については，図２を用いて後述する。

【００１８】監視制御部２４００は，各携帯端末１０００－１，１０００－２，１０００－３の使用状況を監視しており、管理センタ２３００とは異なる方式により、不正使用のチェックを行い，不正使用であると判断される場合には、交換制御局２２００に対して接続を拒否するようにしている。監視制御部２４００の詳細構成については，図６を用いて後述する。

【００１９】次に、図２を用いて、本発明の一実施形態による携帯電話システムにおいて用いる携帯端末１０００の構成について説明する。図２は，本発明の一実施形態による携帯電話システムにおいて用いる携帯端末のブロック図である。

【００２０】携帯端末１０００は、制御部１１００と、記憶部１２００と、変換部１３００と，インタフェース部１４００と，無線回路部１５００と，ベースバンド処理部１６００と，時計１７００とから構成されている。

【００２１】制御部１１００は，携帯端末１０００の全体の制御や、履歴情報算出・格納等を行うものである。記憶部１２００は，携帯端末識別番号と、登録されてい

る携帯端末個々の固定の認証鍵と、履歴情報とを記憶している。ここで、履歴情報については、図４を用いて後述するが、例えば、登録されている携帯端末個々の過去の通話回数，過去の通話相手先電話番号，過去の通話開始時間，過去の通話終了時間，過去の通話時間，過去の通話位置から構成されている。また，記憶部１２００は，制御データや制御手順の情報も記憶している。

【００２２】変換部１３００は，記憶部１２００に記憶されている固定の認証鍵と履歴情報に基づいて，本実施形態による新しい認証鍵を生成する。ここで，履歴情報は，通話の終了時点で，逐次書き換えられるものであるため，新たに生成される認証鍵は，逐次可変の認証鍵となる。従って，従来のような固定の認証鍵の場合に比べて，他人によって不正に取得されにくいものとなり，不正通話もしにくくなるものである。

【００２３】インタフェース部１４００は，携帯端末１０００の入出力部を構成するキー入力を行うキーパッド１８１０と，表示出力を行うディスプレィ１８２０と，着信音等を出力するサウンダ１８３０と，制御部１１００の間の入出力を制御する。

【００２４】無線回路部１５００は，アンテナ１９００によって受信した無線信号を処理する高周波回路部である。ベースバンド処理部１６００は，無線回路部１５００から送られてくる信号を低周波信号に復調して，スピーカー１８５０から音声信号を出力する。また，マイク１８６０から入力された音声信号は，ベースバンド処理部１６００によって変調され，無線回路部１５００によって高周波信号に変換され，アンテナ１９００を介して放射される。

【００２５】時計１７００は，時間を計測し，記憶部１２００に記憶される履歴情報の中の過去の通話開始時間，過去の通話終了時間，過去の通話時間等の時間に関する情報の基準となる時間信号を発生している。

【００２６】なお，各構成要素は，例えば，ＤＳＰ，ＣＰＵ，ＲＯＭ，ＲＡＭ各種ＣＭＯＳ等の電子デバイスにて実現可能である。

【００２７】次に，図３を用いて，本発明の一実施形態による携帯電話システムにおいて用いる管理センタ２３００の構成について説明する。図３は，本発明の一実施形態による携帯電話システムにおいて用いる管理センタのブロック図である。

【００２８】管理センタ２３００は，制御部２３１０と，記憶部２３２０と，変換部２３３０と，インタフェース部２３４０と，時計２３５０とから構成されている。

【００２９】制御部２３１０は，管理センタ２３００の全体の制御や，履歴情報算出・格納等を行うものである。記憶部２３２０は，図２に示した携帯端末１０００の記憶部１２００と同様に，携帯端末識別番号と，登録されている携帯端末個々の固定の認証鍵と，履歴情報と

を記憶している。ここで，履歴情報は，例えば，登録されている携帯端末個々の過去の通話回数，過去の通話相手先電話番号，過去の通話開始時間，過去の通話終了時間，過去の通話時間，過去の通話位置から構成されている。しかしながら，携帯端末１０００の記憶部１２００に記憶されている情報は，個々の携帯端末１０００の情報だけであるのに対して，管理センタ２３００の記憶部２３３０には，全ての携帯端末１０００－１，１０００－２，１０００－３，…の携帯端末識別番号と携帯端末個々の固定の認証鍵と履歴情報の全てが記憶されている。履歴情報は，個々の携帯端末１０００－１，１０００－２，１０００－３，…の通話の終了時点で，逐次書き換えられるものであり，携帯端末１０００の記憶部１２００に記憶される履歴情報と，管理センタ２３００の記憶部２３２０に記憶される履歴情報は，同じものとなっている。また，記憶部２３２０は，制御データや制御手順の情報も記憶している。

【００３０】変換部２３３０は，記憶部２３２０に記憶されている固定の認証鍵と履歴情報に基づいて，本実施形態による新しい認証鍵を生成する。

【００３１】インタフェース部２３４０は，交換制御局２２００との接続を制御する。時計２３５０は，時間を計測し，記憶部２３２０に記憶される履歴情報の中の過去の通話開始時間，過去の通話終了時間，過去の通話時間等の時間に関する情報の基準となる時間信号を発生している。

【００３２】なお，各構成要素は，例えば，ＤＳＰ，ＣＰＵ，ＲＯＭ，ＲＡＭ各種ＣＭＯＳ等の電子デバイスにて実現可能である。

【００３３】次に，図４を用いて，本発明の一実施形態による携帯電話システムにおいて用いる携帯端末及び管理センタ内部の変換部の構成について説明する。図４は，本発明の一実施形態による携帯電話システムにおいて用いる携帯端末及び管理センタ内部の変換部のブロック図である。なお，ここでは，携帯端末１０００の中の変換部１３００を例に取って説明するが，管理センタ２３００の中の変換部２３２０の構成も同様である。

【００３４】変換部１３００には，図２に示した記憶部１２００から履歴情報と固定の認証鍵が入力する。履歴情報としては，携帯端末の過去の通話回数１２１０と，過去の通話相手先電話番号１２２０と，過去の通話開始時間１２３０と，過去の通話終了時間１２４０と，過去の通話時間１２５０と，過去の通話位置１２６０とから構成されているものとする。

【００３５】携帯端末の過去の通話回数１２１０は，携帯端末が使用可能になってからの過去の全通話回数であり，Ｎ１ビットの情報で表される。制御部１１００は，通話毎に最新の通話回数１２１０をインクリメントし，記憶部１２００に格納する。過去の通話相手先電話番号１２２０は，通話毎に交換制御局２２００（図１）より

転送されてくる情報であり．N2ビットの情報で表される。制御部1100は、通話毎に最新の通話相手先電話番号1220を記憶部1200に格納する。

【0036】過去の通話開始時間1230，通話終了時間1240，及び通話時間1250は．通話開始・終了時に時計1700で得られる通話接続年月日・時刻情報であり、それぞれN3ビット，N4ビット，N5ビットの情報で表される。制御部1100は．通話毎に最新の過去の通話開始時間1230，通話終了時間1240，通話時間1250を記憶部1200に格納する。

【0037】過去の通話位置1260は、携帯端末を使った位置特定システムによって得られる位置情報であり．N6ビットの情報で表される。PHSを使う位置特定システムについては、例えば、日経エレクトロニクス．1996.7.15，(no.666)に記載されている。図1に示した特定の携帯端末1000－1と．複数の基地局2100A，2100B，2100Cの間の接続は．携帯端末1000－1からの信号を受信した複数の基地局2100A，2100B，2100Cの信号強度を．交換制御部2200が判断して．最も電界強度の大きな基地局との間で成立するように制御される。従って．もし、基地局2100Aが受信する携帯端末1000－1から電界強度が最も大きいときには、基地局2100Aが交換制御部2200によって選択される。携帯端末1000が移動する際には、どの移動に応じて基地局2100の順次最も電界強度の大きい基地局に切換えられる。従って．通話終了時において．接続されていた基地局2100を、過去の通話位置1260として、制御部1100は．通話毎に最新の過去の通話位置1260を記憶部1200に格納する。

【0038】さらに、固定の認証鍵1270は．N7ビットで表されるものとする。

【0039】ここで、携帯端末の過去の通話回数1210（N1ビット）と、過去の通話相手先電話番号1220（N2ビット）と、過去の通話開始時間1230（N3ビット）と．通話終了時間1240（N4ビット）と．通話時間1250（N5ビット）と、過去の通話位置1260（N6ビット）と、固定の認証鍵1270（N7ビット）の合計ビット数を、128ビットとする。この128ビットのパラレルデータが、変換部1300に取り込まれる。

【0040】変換部1300は、2個の疑似乱数発生回路1310，1320と．論理和回路1330とから構成されている。疑似乱数発生回路1310，1320は．例えば、岡本著，「暗号理論入門」，共立出版に記載されているようなフィードバックシフトレジスタによる疑似乱数発生回路である。疑似乱数発生回路1310には．記憶部1200から取り込まれた128ビットのデータの内の下位の64ビットのパラレルデータが初期設定される。また、疑似乱数発生回路1320には、記

憶部1200から取り込まれた128ビットのデータの内の上位の64ビットのパラレルデータが初期設定される。疑似乱数発生回路1310，1320は、設定されたデータの排他論理和を演算して、1ビットデータを生成し．さらに．1ビット分だけシフトした上で．排他論理和を演算して．次の1ビットデータを生成するというように、64ビットのシリアルデータを出力する。疑似乱数発生回路1310，1320の出力するシリアルデータは、論理和回路1330によって演算され．64ビットのシリアルデータとして出力される。

【0041】即ち、変換部1300は．入力した128ビットのデータを、2分割した上で．それぞれのデータに基づいて、所定の論理演算を行い．64ビットのデータとして出力するものである。入力するデータが．128ビットよりも少ない場合には、所定の冗長ビットを付加して、128ビット構成とし、128ビットよりも多い場合には、所定のビットを削除して．128ビット構成とすることができる。また、ビット構成は、128ビットから64ビットに変換するだけでなく、他の任意ビットの変換を行うようにすることができる。また．シフトレジスタを用いた疑似乱数発生回路以外のハード構成を持つものでもよく、さらに、ソフトウエアにより同様の機能を達成するものであってもよい。

【0042】本実施形態においては．従来から用いられている固定の認証鍵1270以外に．逐次書き換えられる履歴情報1210，1220，1230，1240，1250，1260を用いて、新たな認証鍵を生成するようにした点に特徴があるものである。

【0043】次に、図5を用いて、本発明の一実施形態による携帯電話システムにおける認証実行手順について説明する。図5は、本発明の一実施形態による携帯電話システムにおいて用いる携帯端末及び管理センタにおける認証実行手順を示すフローチャートである。

【0044】図5に示す例では、基地局2100に接続しようとしている携帯端末1000が．接続を許された正当な携帯端末であるか否かを認証するものである。

【0045】ステップ501において．携帯端末1000のユーザが．相手先の電話番号を押し電話をかけると．携帯端末1000は．記憶部1200に記憶されている携帯端末識別番号を．管理センタ2300へ基地局2100経由で転送する。

【0046】ステップ521において．管理センタ2300は、転送されてきた携帯端末識別番号が前もって登録されているか確認を行い．登録されていれば．転送されてきた携帯端末識別番号に対応する履歴情報及び固定の認証鍵を記憶部2320から検索する。

【0047】次に、ステップ502において、携帯端末1000の変換部1300は、また．ステップ522において、管理センタ2300の変換部2320は．図4において説明したようにして、新しい認証鍵を生成す

る。

【００４８】ステップ５２３において．管理センタ２３００の制御部２３１０は．携帯端末１０００に対して、基地局２１００経由で認証用データＡを転送する。

【００４９】ステップ５０３において．携帯端末１０００の制御部１１００は、ステップ５０２において生成した新しい認証鍵に基づいて．管理センタ２３００から送られてきた認証用データＡを、認証応答ａに変換する。この変換自体は．従来から行われている認証用データＡを．個々の携帯端末に予め設定されている認証鍵を用いて認証応答ａに変換するのと同様である。本実施形態においては、変換に使用する認証鍵が．従来とは相違するものである。

【００５０】同様にして．ステップ５２４において、管理センタ２３００の制御部２３１０は．ステップ５２２で生成した新しい認証鍵に基づいて．認証用データＡを認証子ａ'に変換する。

【００５１】次に、ステップ５０４において、携帯端末１０００の制御部１１００は、無線回路部１５００を経由して、認証応答ａを、管理センタ２３００へ基地局２１００経由で転送する。

【００５２】ステップ５０５において．携帯端末１０００は．サービス応答待ちになる。

【００５３】一方、ステップ５２５において、管理センタ２３００の制御部２３１０は、携帯端末１０００から転送されてきた認証応答ａと、ステップ５２４において管理センタ２３００自身で作成した認証子ａ'を比較する。

【００５４】ステップ５２６において．管理センタ２３００は、ステップ５２５における比較結果が一致するか否かを判断する。

【００５５】一致した場合には、ステップ５２７において．管理センタ２３００は．交換制御部２２００に通話を許可し、一致しない場合には、ステップ５２８において．管理センタ２３００は．交換制御部２２００に通話を拒否する。

【００５６】なお、携帯端末の個々の過去の履歴情報や携帯端末個々に割り当てられている識別番号を格納してある記憶部の内容をダウンロードして不正を行うような場合もありうるので、そのような場合の対策としては、図２に、破線で示す不正開放検出手段１２８０と消去回路１２９０を設ければよいものである。不正開放検出手段１２８０は．例えば、携帯端末の筐体を止める複数のビスを所定の順番で緩めないと、電源電圧の信号を出力するものである。消去回路１２９０は．不正開放検出手段１２８０の信号に基づいて、例えば．ＥＥＰＲＯＭから構成される記憶部１２００の記憶内容を消去するようにすればよいものである。

【００５７】なお、以上の説明では．記憶部に記憶された履歴情報の書換は、各通話の終了毎に行うものとしたが．複数回の通話毎に行うようにしてもよく、また、携帯端末のユーザの要求に応じて行うようにしてもよいものである。

【００５８】本実施形態によれば、従来の個々の携帯端末に予め割当られている認証鍵に加えて、逐次書き換えられる履歴情報を用いて．新しい認証鍵を生成するようにしているため．不正使用を防止し得るものとなる。

【００５９】次に、図６及び図７を用いて、本発明の第２の実施形態による携帯電話システムについて説明する。最初に、図６を用いて．本発明の第２の実施形態による携帯電話システムの監視制御部について説明する。図６は、本発明の第２の実施形態による携帯電話システムの監視制御部のブロック図である。

【００６０】本実施形態においても．携帯電話システムの全体構成は．図１に示したものと同様である。本実施形態においては．図１に示した監視制御部２４００を用いて．不正使用をチェックするようにしているものである。

【００６１】監視制御部２４００は．制御部２４１０と．記憶部２４２０と、インタフェース部２４４０と、時計２４５０とから構成されている。

【００６２】制御部２４１０は、監視制御部２４００の全体の制御や．記憶部２４２０のアクセス及び通話料金や通話位置によって携帯端末の不正使用を検出するものである。記憶部２４２０は．携帯端末ユーザの通話料金の上限，ユーザの前回の通話位置及び通話終了時間等を格納する。

【００６３】インタフェース部２４４０は、交換制御局２２００との接続を制御する。時計２４５０は．時間を計測し、記憶部２４２０に記憶される履歴情報の中の前回の通話時間等の時間に関する情報の基準となる時間信号を発生している。

【００６４】なお、各構成要素は、例えば、ＤＳＰ，ＣＰＵ．ＲＯＭ．ＲＡＭ各種ＣＭＯＳ等の電子デバイスにて実現可能である。

【００６５】監視制御部２４００は．携帯端末ユーザの通話料金や通話位置によって携帯端末の不正使用を検出する装置であり．管理センタ２３００は携帯端末の認証を行うだけの装置である。監視制御部２４００と管理センタ２３００は．別々の装置であっても良いし．同一の装置であっても良い。

【００６６】次に、図７を用いて、本発明の第２の実施形態による携帯電話システムの監視制御部における携帯端末の不正使用の検出手順について説明する。図７は、本発明の第２の実施形態による携帯電話システムの監視制御部における携帯端末の不正使用の検出手順を示すフローチャートである。

【００６７】ステップ７００において．監視制御部２４００の記憶部２４２０に．ユーザ毎に．月毎の通話料金の上限及び日毎の通話料金の上限を登録する。

【００６８】次に、ステップ７０１において、監視制御部２４００の制御部２４１０は、日毎及び月毎に通話料金を監視し、ユーザ毎の通話料金が予め登録しておいた通話料金の上限を越えているかチェックする。

【００６９】ステップ７０２において、監視制御部２４００の制御部２４１０は、日毎及び月毎に通話料金が、ユーザ毎の通話料金が予め登録しておいた通話料金の上限を越えているか否かを判断し、越えていない場合には、正当な使用であると判断して、ステップ７０２に戻る。越えている場合には、不正な使用であるとして、ステップ７０４に進む。

【００７０】ステップ７０４において、監視制御部２４００の制御部２４１０は、管理センタ２３００へ、このユーザの携帯端末使用停止命令のコマンドを送る。

【００７１】次に、ステップ７０５において、管理センタ２３００は、このユーザの携帯端末使用停止命令のコマンドを受け取ると、ユーザの携帯端末識別番号及び認証鍵を抹消する。この操作によって、ユーザの携帯端末は、認証が正当に行われなくなるため、携帯端末の使用ができなくなる。

【００７２】なお、以上の説明では、正当使用者が、料金の上限を越えて使用する場合にも、ユーザの携帯端末識別番号及び認証鍵が抹消されることになるので、かかる事態を避けるためには、ステップ７０３において、上限を越えていると判断された場合には、予め、携帯端末のユーザに対して、上限値を越えた旨通知するようにしてもよいものである。

【００７３】本実施形態によれば、監視制御部によって、通話料金をチェックすることにより、容易に、不正通話を防止し得るものとなる。

【００７４】次に、図８を用いて、本発明の第３の実施形態による携帯電話システムの監視制御部における携帯端末の不正使用の検出手順について説明する。図８は、本発明の第３の実施形態による携帯電話システムの監視制御部における携帯端末の不正使用の検出手順を示すフローチャートである。

【００７５】なお、本実施形態においても、携帯電話システムの全体構成は、図１に示したものと同様であり、また、監視制御部２４００の構成は、図６において説明したものと同様である。本実施形態においては、図６に示した監視制御部２４００を用いて、不正使用をチェックするようにしているものである。

【００７６】ステップ８０１において、監視制御部２４００の制御部２４１０は、通話開始時もしくは通話中もしくは通話終了時に、時計２４５０によって得られる時刻情報と、携帯端末を使った位置特定システムによって得られる位置情報を記憶部２４２０へユーザ別に格納する。

【００７７】次に、ステップ８０２において、監視制御部２４００の制御部２４１０は、通話毎に通話開始時もしくは通話中もしくは通話終了時に、時計２４５０によって得られる時刻情報と、携帯端末を使った位置特定システムによって得られる位置情報を得て、今回の時刻情報と前回の時刻情報との差が予め設定した一定の時刻T以内であり、かつ、今回の通話位置と前回の通話位置との差が予め設定した一定の距離D以上離れているかをチェックする。

【００７８】ステップ８０３において、監視制御部２４００の制御部２４１０は、ステップ８０２におけるチェック結果を判断して、ＹＥＳであれば、不正な使用であるとして、ステップ８０４に進み、ＮＯであれば、正当な使用であるとして、ステップ８０２に戻る。

【００７９】ステップ８０３において、ＹＥＳである場合とは、例えば、１月１日の午前９時に携帯端末が、東京にある基地局の管内で使用され、同一の識別番号を有する携帯端末が、同日の午前９時５分に、北海道にある基地局の管内で使用された場合等が該当する。即ち、通常の携帯端末の使用状況からして、時間的、空間的に、同一の識別番号を有しながら、異なる携帯端末が使用されたような状況を識別するようにしている。ここで、予め設定しておくべき時刻情報Ｔと位置情報Ｄは携帯端末全てのユーザに共通であっても、個々に異なってもよい。

【００８０】ステップ８０４において、監視制御部２４００の制御部２４１０は、管理センタ２３００へ、ユーザの携帯端末使用停止命令のコマンドを送る。

【００８１】次に、ステップ８０５において、管理センタ２３００は、ユーザの携帯端末使用停止命令のコマンドを受け取ると、管理センタ２３００の記憶部２３２０からこのユーザの携帯端末識別番号及び認証鍵を抹消する。この操作によって、ユーザの端末認証が正当に行われなくなるため、携帯端末の使用ができなくなる。

【００８２】なお、正当使用者に対しては、携帯端末識別番号及び認証鍵を抹消した旨を通知する。

【００８３】本実施形態によれば、監視制御部によって、通話開始時間及び通話位置をチェックすることにより、容易に、不正通話を防止し得るものとなる。

【００８４】

【発明の効果】本発明によれば、不正通話を防止し得るものとなる。

【図面の簡単な説明】

【図１】本発明の一実施形態による携帯電話システムのブロック図である。

【図２】本発明の一実施形態による携帯電話システムにおいて用いる携帯端末のブロック図である。

【図３】本発明の一実施形態による携帯電話システムにおいて用いる管理センタのブロック図である。

【図４】本発明の一実施形態による携帯電話システムにおいて用いる携帯端末及び管理センタ内部の変換部のブロック図である。

13　　14

【図５】本発明の一実施形態による携帯電話システムにおいて用いる携帯端末及び管理センタにおける認証実行手順を示すフローチャートである。

【図６】本発明の第２の実施形態による携帯電話システムの監視制御部のブロック図である。

【図７】本発明の第２の実施形態による携帯電話システムの監視制御部における携帯端末の不正使用の検出手順を示すフローチャートである。

【図８】本発明の第３の実施形態による携帯電話システムの監視制御部における携帯端末の不正使用の検出手順を示すフローチャートである。

【符号の説明】

１０００…携帯端末

１１００…制御部

＊１２００…記憶部

１３００…変換部

１３１０，１３２０…疑似乱数発生回路

２１００…基地局

２２００…交換制御局

２３００…管理センタ

２３１０…制御部

２３２０…記憶部

２３３０…変換部

２４００…監視制御局

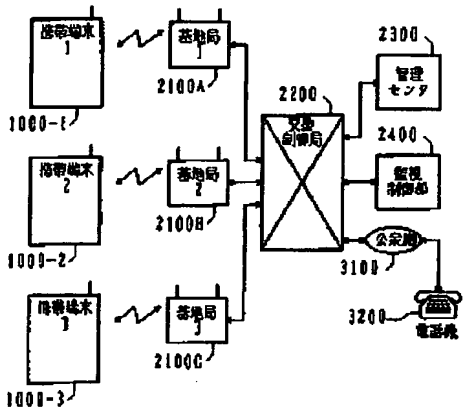
２４１０…制御部

２４２４…記憶部

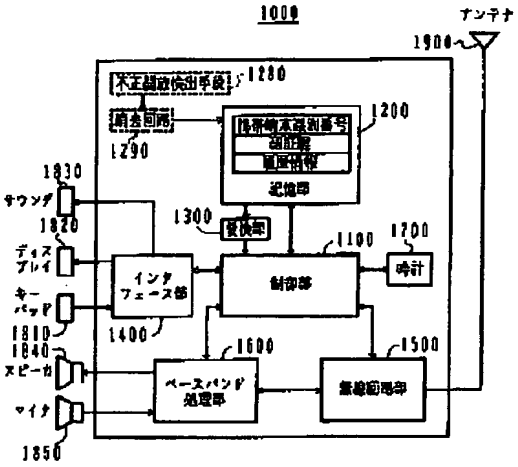
３１００…公衆網

＊　３２００…電話機

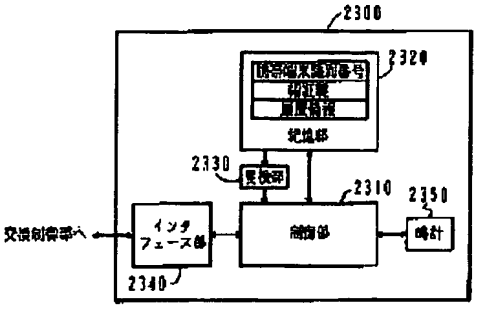
【図１】



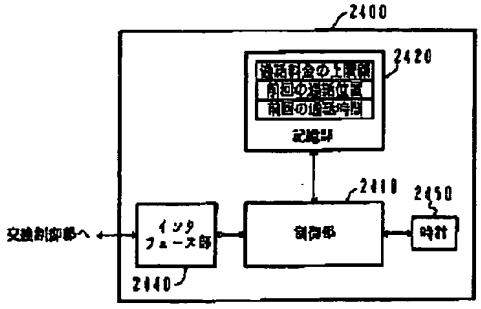
【図２】



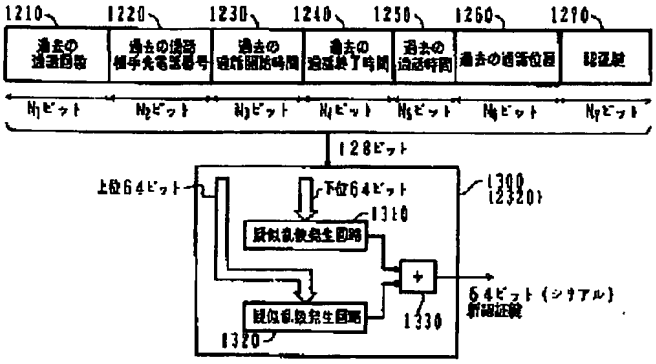
【図３】



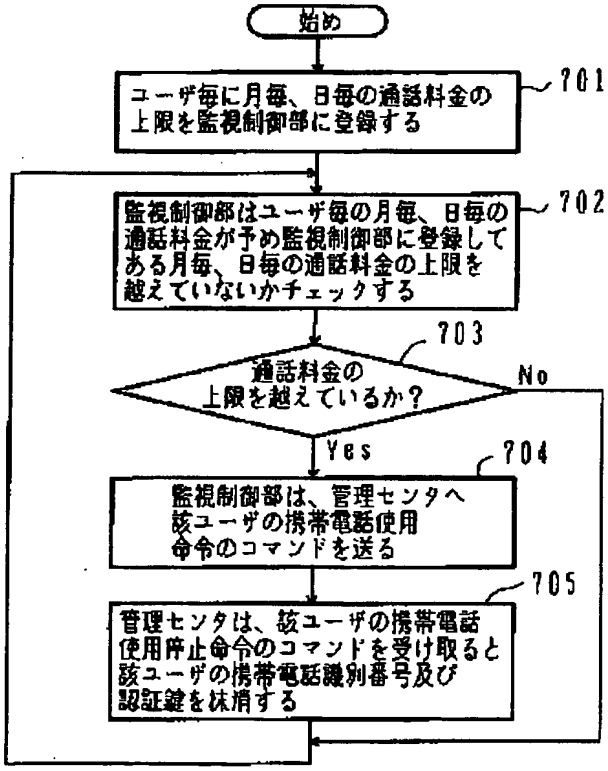
【図６】



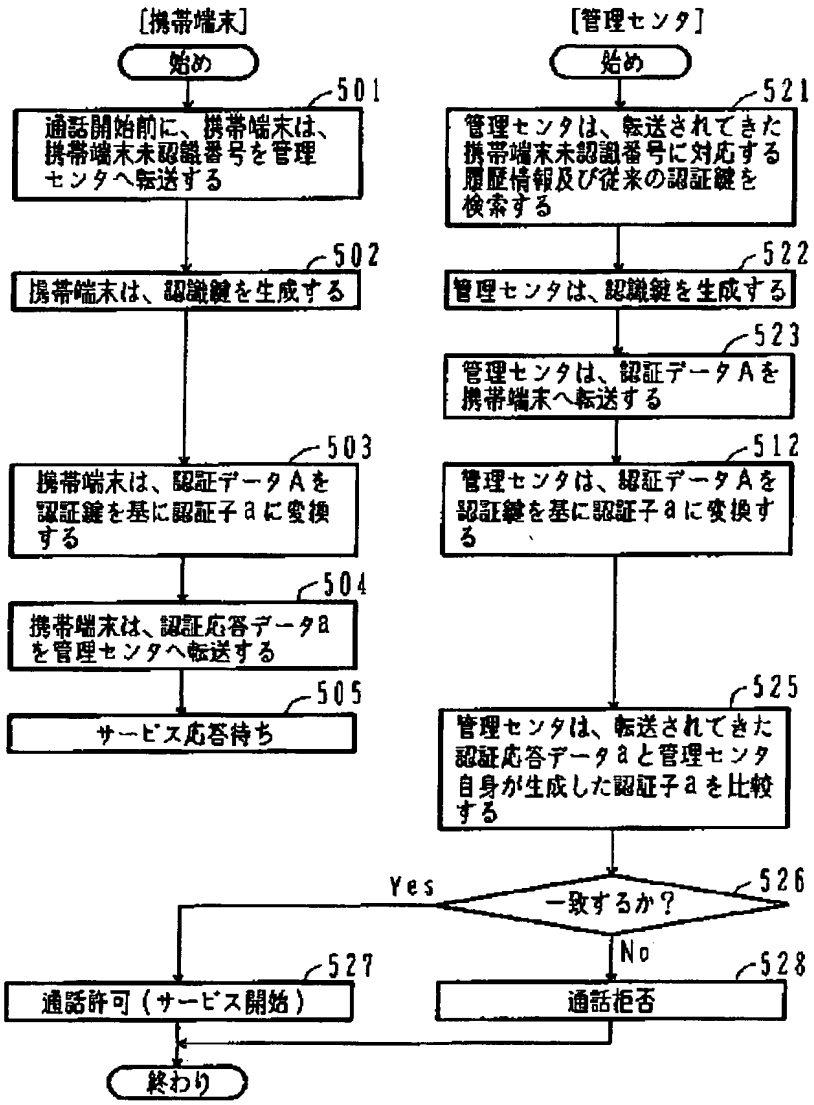
【図4】



【図7】



【図5】



【図8】